



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,252	01/17/2001	James Russell Godwin	5577-220	8043

58505 7590 10/27/2006  
STEVENS & SHOWALTER, L.L.P.  
BOX IBM  
7019 CORPORATE WAY  
DAYTON, OH 45459-4238

EXAMINER

PATEL, ASHOKKUMAR B

ART UNIT PAPER NUMBER

2154

DATE MAILED: 10/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/764,252	<b>Applicant(s)</b> GODWIN ET AL.	
	<b>Examiner</b> Ashok B. Patel	<b>Art Unit</b> 2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 15 August 2006.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-72 is/are pending in the application.  
4a) Of the above claim(s) 2, 10-19, 21, 29-38, 40 and 48-57 is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1, 3-9, 20, 22-28, 39, 41-47 and 58-72 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 1-72 are subject to examination. Claims 2, 10-19, 21, 29-38, 40 and 48-57 have been cancelled.

**Response to Arguments**

2. Applicant's arguments with respect to claims 1, 20 and 39 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

- a. Claim 1, 3-9, 20, 22-28, 39, 41-47, 58-72 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "to distribute workload associated with the network communications among the target hosts" in lines 18 and 19 of the claim 1. The same claim also recites "an end-to-end secure network communications through the distribution processor", "outbound and inbound communications", network communications directed to common address", preamble recites "secure communications", "inbound and outbound end-to-end network communications", "security processing of communications" and " the received network communications".

Which type and how all of these type of “communications” associated with “the network communications”? What type of “communication is represented by “the network communications”?

There is insufficient antecedent basis for this limitation in the claims.

Claim 1 also recites “the selection among the target hosts” in line 17, also at the same time claim recites “selected ones of the plurality of target hosts are associated with the end-to-end secure network communications”, “the received network communications that are directed to the common address among selected ones of the target hosts”, as well as the preamble recites “providing secure communications over a network”

Which type, and how all of these type of “selection” and “target hosts” associated with “the selection among the target hosts ”?

There is insufficient antecedent basis for this limitation in the claims.

For the purpose of this office action, the claim is interpreted as follows:

The communications are received and delivered from the distribution processor to the target hosts wherein the distribution processor receives network communications directed to the common network address, and selection among the host for workload distribution is carried out so as to distribute workload associated with the network communications. Also, as preamble declares, the method provides secure communications over a network in a distributed workload environment having target hosts, and as such, there is no selection of whether the communication requires non-

Art Unit: 2154

secure communications, and also as such, the selection of target hosts is associated with the "distribution of workload associated with the network communication."

Please note that claim 3 presents the determination of the received network communications whether the received network communication is end-to-end secure network communication" or "not end-to-end secure network communication."

Although, the preamble of claim 1 is applicable to claim 3 and claim 3's dependent claim 4 as interpreted above, claim 3 is being examined as it recites. This is also applicable to claims 22, 23, 41 and 42 as these claims to system that carries out the method of claims 3 and 4 and computer readable medium having computer readable program code that carries out the method of claims 3 and 4.

Claims 3-9, 54-60 and 64-66 are also rejected along with claim 1 because of their dependency on claim 1.

Claim 20 is a claim to a system that carries out the method of claim 1 and also recite the same claim language as claim 1. Therefore claim 20 is also rejected for the reasons set forth for claim 1.

Claims 22-28 and 67-69 are also rejected along with claim 20 because of their dependency on claim 20.

Claim 39 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 1 and also recite the same claim language as claim 1. Therefore, claim 39 is rejected for the reasons set forth for claim 1.

Art Unit: 2154

Claims 41-47, 61-63 and 70-72 are also rejected along with claim 20 because of their dependency on claim 20.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless-

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 7, 20, 26, 39, 45 and 58-72 are rejected under 35 U.S.C. 102(e) as being anticipated by Bhaskaran (US 6, 266, 335 B1).

**Referring to claim 1,**

Bhaskaran teaches a method for providing secure communications (col. 2, line 66-col. 3, line 3, "There is thus a need for a system that not only allows for transmissions of encrypted data packets according to the IPSEC model, but also allows network administrators to perform both server load balancing and IPSEC in their networks.", col. 6, line 48-50) over a network in a distributed workload environment having target hosts which are accessed through a distribution processor (col. 4, line 19-28, "In some embodiments, the network flow switch, in addition to routing of the packets, performs load balancing and fault tolerance functions. In these embodiments, a processor of the network flow switch periodically executes a load balancing routine to determine the relative workload of each of the IP servers. When the network flow

Art Unit: 2154

switch receives a packet destined to the cluster of IP servers, the packet is routed to the IP server with an optimal workload, so as to ensure that the workload is evenly distributed among the IP servers.”) by a common network address (col.3, line 45-49, “The present invention provides a network flow switch (and a method of operation thereof)for connecting a pool of IP routers to a cluster of IP servers sharing a single IP address, without requiring translation of the IP address, and providing bi-directional clustering.”), the method comprising the steps of:

routing both inbound and outbound communications with target hosts (col.3, line 45-49, “The present invention provides a network flow switch (and a method of operation thereof)for connecting a pool of IP routers to a cluster of IP servers sharing a single IP address, without requiring translation of the IP address, and providing bi-directional clustering.”) which are associated with an end-to-end secure network communication (col. 6, line 48-50, Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken.”) through the distribution processor (col. 5, line 47-51, “A cluster of IP servers 200 and a network flow switch 205, according to an embodiment of the invention, are shown in FIG. 2. Network flow switch 205 routes packets among IP servers 210, 220, 230,240 and 250 and network routers 260, 270 and 280.”);

processing both inbound and outbound end-to-end secure network communications at the distribution processor (col. 5, line 47-51, “A cluster of IP servers 200 and a network flow switch 205, according to an embodiment of the invention, are shown in FIG. 2. Network flow switch 205 routes packets among IP servers 210, 220,

Art Unit: 2154

230,240 and 250 and network routers 260, 270 and 280.”)so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host (col. 6, line 48-50, Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken.”);

receiving at file distribution processor, network communications directed to the common network address (col.3, line 45-49, “The present invention provides a network flow switch (and a method of operation thereof)for connecting a pool of IP routers to a cluster of IP servers sharing a single IP address, without requiring translation of the IP address, and providing bi-directional clustering.”);

encapsulating communications between the distribution processor (col. 6, line 48-50, Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken.”) and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications col. 4, line 19-28, “In some embodiments, the network flow switch, in addition to routing of the packets, performs load balancing and fault tolerance functions. In these embodiments, a processor of the network flow switch periodically executes a load balancing routine to determine the relative workload of each of the IP servers. When the network flow switch receives a packet destined to the cluster of IP servers, the packet is routed to the IP server with an optimal workload, so as to ensure that the workload is evenly distributed among the IP servers.”); and



Art Unit: 2154

distributing the received network communications that are directed to the common network address (col.3, line 45-49, "The present invention provides a network flow switch (and a method of operation thereof)for connecting a pool of IP routers to a cluster of IP servers sharing a single IP address, without requiring translation of the IP address, and providing bi-directional clustering.")among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts (col. 7, line 32-37, "Stage 435 performs an optional load balancing operation to determine which of IP servers 210, 220, 230, 240 or 250 packet 300 is to be routed to. The load balancing operation of stage 435 attempts to divide packets to be processed among the IP servers according to the capacity and the current utilization of each server.", Please note that flow switch is distributing workload among the IP servers per packet basis, and as such, the flow switch has to establish IPSEC tunnel with the selected IP servers to which it distributes the workload.)

**Referring to claim 7,**

Bhaskaran teaches a method according to Claim 1, wherein the communications received from the target hosts at the distribution processor and the encapsulated communications to ones of the plurality of target hosts from the distribution processor are communicated over trusted communication links. (col. 6, line 48-50, Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken.", col. 7, line 32-37, "Stage 435 performs an optional load balancing operation to determine which of IP servers 210, 220, 230, 240 or 250 packet

Art Unit: 2154

300 is to be routed to. The load balancing operation of stage 435 attempts to divide packets to be processed among the IP servers according to the capacity and the current utilization of each server.”, Please note that flow switch is distributing workload among the IP servers per packet basis, and as such, the flow switch has to establish IPSEC tunnel with the selected IP servers to which it distributes the workload.)

**Referring to claim 20,**

Claim 20 is a claim to a system that carries out the method of claim 1. Therefore, claim 20 is rejected for the reasons set forth for claim 1. (please note that means are identified in claim 1, in col. 3, line 45-49, col. 6, line 4850, and col. 4, line 22-25).

**Referring to claim 26,**

Claim 26 is a claim to a system that carries out the method of claim 7. Therefore, claim 26 is rejected for the reasons set forth for claim 7.

**Referring to claim 39,**

Claim 39 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 1. Therefore, claim 39 is rejected for the reasons set forth for claim 1.

**Referring to claim 45,**

Claim 45 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 7. Therefore, claim 45 is rejected for the reasons set forth for claim 7.

**Referring to claim 58,**

Bhaskaran teaches the method according to claim 1, wherein distributing the received network communications that directed to the common IP address among selected ones of the target hosts comprises:

Selecting among the target hosts for distribution of the network communications in response to a predefined selection pattern to distribute workload associated with the network communications among the target hosts.(col. 8, line 29-34)

**Referring to claim 59,**

Bhaskaran teaches the method of claim 58, wherein selecting among the target hosts for distribution of the network communications in response to a predefined selection pattern to distribute workload associated with the network communications among the target hosts comprises selecting among the target hosts associated with the common network address based on a round-robin pattern. (col. 8, line 29-34, "The network flow switch intercepts the request, examines the IP server's IP address, and responds to the request by assigning the Data Link Layer address of the network router in the pool that is best able to service the load coming from this particular server ("best" is determined by measures of real time traffic load or using a simple round robin scheme based on server source IP addresses).")

**Referring to claim 60,**

Bhaskaran teaches the method according to claim 1, wherein distributing the received network communications that directed to the common network address among selected ones of the target hosts comprises: Selecting among the target hosts for distribution of the network communications in response to a dynamic criteria that

Art Unit: 2154

changes over a time to distribute workload associated with the network communications among the target hosts (col. 8, line 29-34, "The network flow switch intercepts the request, examines the IP server's IP address, and responds to the request by assigning the Data Link Layer address of the network router in the pool that is best able to service the load coming from this particular server ("best" is determined by measures of real time traffic load or using a simple round robin scheme based on server source IP addresses).")

**Referring to claim 61,**

Claim 61 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 58. Therefore, claim 61 is rejected for the reasons set forth for claim 58.

**Referring to claim 62,**

Claim 62 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 59. Therefore, claim 62 is rejected for the reasons set forth for claim 59.

**Referring to claim 63,**

Claim 63 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 60. Therefore, claim 63 is rejected for the reasons set forth for claim 60.

**Referring to claim 64,**

Bhaskaran teaches the method according to claim 1, further comprising: receiving at a target host, an encapsulated communication; comparing a physical link

Art Unit: 2154

corresponding to said distributor to a source of encapsulation; ignoring the encapsulated communication if said physical link does not match to said source of encapsulation. (col. 6, line 48-50, Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken.”);

**Referring to claim 65,**

Bhaskaran teaches the method according to claim 1, wherein distributing the received network communications that are directed to the common network address among selected ones of the target hosts distribution processor comprises distributing the received network communications using a sysplex distributor. ( col. 5, line 47-col. 6, line 2, “A cluster of IP servers 200 and a network flow switch 205, according to an embodiment of the invention, are shown in FIG. 2. Network flow switch 205 routes packets among IP servers 210, 220, 230,240 and 250 and network routers 260, 270 and 280. IP servers 210, 220, 230,240 and 250 are configured identically and have a virtual IP address 290. In addition, each of IP servers 210, 220, 230, 240 and 250 has a distinct Data Link Layer address, and a distinct link name. The link name is used to identify the unique server within the cluster of servers sharing a same IP address. As explained below, the Data Link Layer address is used to translate a virtual Data Link Layer address to a physical Data Link Layer address, after an IP server is selected by network flow switch 205 to receive the packet. IP address 290 is visible to devices communicating with the cluster 200, while the individual Data Link Layer addresses of each of the IP servers are not. Network flow switch 205, in fact, performs a proxy Address Resolution Protocol (ARP) function that returns a "virtual" Data Link Layer

Art Unit: 2154

address (not shown) to a network connected device in response to a standard ARP query. As a result, network connected devices see the cluster 200 as having a single IP address 290 and a single Data Link Layer address (not shown).")

**Referring to claim 66,**

Bhaskaran teaches method according to claim 1, wherein the end-to-end secure network communication comprises a communication using the IPSEC communication protocol. (col. 6, line 48-50, Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken.")

**Referring to claim 67,**

Claim 67 is a claim to a system that carries out the method of claim 64. Therefore, claim 67 is rejected for the reasons set forth for claim 64.

**Referring to claim 68,**

Claim 68 is a claim to a system that carries out the method of claim 65. Therefore, claim 68 is rejected for the reasons set forth for claim 65.

**Referring to claim 69,**

Claim 69 is a claim to a system that carries out the method of claim 66. Therefore, claim 69 is rejected for the reasons set forth for claim 66.

**Referring to claim 70,**

Claim 70 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 64. Therefore, claim 70 is rejected for the reasons set forth for claim 64.

**Referring to claim 71,**

Claim 71 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 66. Therefore, claim 71 is rejected for the reasons set forth for claim 66.

**Referring to claim 72,**

Claim 72 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 66. Therefore, claim 72 is rejected for the reasons set forth for claim 66.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 3-6, 8, 9, 22-25, 27, 28, 41-44, 46 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhaskaran (US 6, 266, 335 B1). in view Shaffer et al. (hereinafter Shaffer) (US 6, 826, 599 B1)

**Referring to claim 3,**

Keeping in mind the teachings of Bhaskaran as stated in claim 1 above, Bhaskaran fails to teach a method according to Claim 1, further comprising the steps of: determining if the received network communications are end-to-end secure network communications which are to be distributed to ones of the target hosts; wherein encapsulating communications between the distribution processor and selected ones of

Art Unit: 2154

the plurality of target hosts which are associated with end-to-end secure network communications comprises processing the received network communications so as to provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are end-to-end secure network communications which are distributed to ones of the target hosts and to not provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are not end-to-end secure network communications.

Shaffer teaches at col. 5, line 45 -col. 6, line 13, "During normal operation, a client platform 100 transmits a request to retrieve data such as, for example, a multimedia object from destination platform 106. Cache-enabled router 102 receives the request in the form of at least one data packet. Router 102 reads the packet header to determine whether, for example, it is a TCP packet and indicates port 80 as its destination port. If the packet is of a different protocol or is not destined for the World Wide Web, the packet is simply passed through the router and routed according to standard Internet protocols. If, on the other hand, the packet is TCP and port 80 is specified, router 102 determines to which of its associated network caches (108 and 110) it will redirect the packet based on the destination IP address specified in the packet. Before sending the packet to one of its associated network caches, router 102 encapsulates the packet for transmission to the selected network cache by adding another TCP/IP header which designates the router as the source of the packet and the network cache as the destination. That is, the router encapsulates the packet for transmission to a network cache which might be several "hops" away. So, for example,



Art Unit: 2154

router 102 might encapsulate the packet for transmission to network cache 114 which is connected to router 102 via router 112. Thus, not only may multiple network caches be associated with a particular router, but multiple routers may be supported by an individual network cache or a group of network caches. This allows a tremendous amount of flexibility in where the network cache and router need to be in relation to each other. It will, of course, be understood that the present invention is not limited to port 80 or any particular packet encapsulation scheme (e.g., GRE, MAC, etc.) A TCP connection is established between the client and the selected network cache and router 102 transmits the encapsulated packet to the network cache.”

Thereby Shaffer teaches a concept that is of a paramount importance to one having ordinary skill in the art. And that that a device can determine whether to apply any encapsulation scheme to the incoming communication by reading the packet header to determine whether, for example, it is a TCP packet. If the packet is of a different protocol or is not destined for the World Wide Web, the packet is simply passed through and routed according to standard Internet protocols. Port 80 and encapsulation scheme are not limitations for applying the concept and technique taught by Shaffer. Thus Shaffer teaches determining if the received network communications are end-to-end secure network communications which are to be distributed to ones of the target hosts; wherein encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications comprises processing the received network communications so as to provide encapsulated generic communications to the ones of

the plurality of target hosts if the received network communications are end-to-end secure network communications which are distributed to ones of the target hosts and to not provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are not end-to-end secure network communications.

Therefore, it would have been an obvious to one of an ordinary skill in art, having the teachings of Bhaskaran and Shaffer in front of him at the time of invention was made, to implement the technique of Shaffer to the flow switch of Bhaskaran such that which can be implemented regardless of the port as well as encapsulation scheme, such as GRE, IPSEC, to selectively send the packets to the server for the network communications requiring end-to-end secure network communications along with the load balancing. If the network communication does not require end-to-end secure network communications there is saving in the consumption of valuable processing resources at the flow switch as well as at the destination server level.

**Referring to claim 4,**

Bhaskaran teaches a method according to Claim 3, wherein-the-step-of processing both inbound and outbound end-to-end secure network communications further comprises the steps of: receiving at the distribution processor communications from the ones of the target hosts which are associated with end-to-end secure network communications; and processing the received communications from the ones of the target hosts so as to provide endpoint network security for the communications from the ones of the target hosts. (col. 6, line

Art Unit: 2154

48-50, Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken.”, col. 7, line 32-37, “Stage 435 performs an optional load balancing operation to determine which of IP servers 210, 220, 230, 240 or 250 packet 300 is to be routed to. The load balancing operation of stage 435 attempts to divide packets to be processed among the IP servers according to the capacity and the current utilization of each server.”, Please note that flow switch is distributing workload among the IP servers per packet basis, and as such, the flow switch has to establish IPSEC tunnel with the selected IP servers to which it distributes the workload.)

**Referring to claims 5 and 6,**

Bhaskaran teaches a method according to Claim 1, wherein encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications comprises encapsulating the communications (col. 6, line 48-50, Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken.”, col. 7, line 32-37, “Stage 435 performs an optional load balancing operation to determine which of IP servers 210, 220, 230, 240 or 250 packet 300 is to be routed to. The load balancing operation of stage 435 attempts to divide packets to be processed among the IP servers according to the capacity and the current utilization of each server.”, Please note that flow switch is distributing workload among the IP servers per packet basis, and as such, the flow switch has to establish IPSEC tunnel with the selected IP servers to which it distributes the workload.)

Bhaskaran fails to teach encapsulation in a generic routing format method according to claim 5, wherein the generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distribution processor and ones of the plurality of target hosts..

Shaffer teaches at col. 5, line 45 -col. 6, line 13, "During normal operation, a client platform 100 transmits a request to retrieve data such as, for example, a multimedia object from destination platform 106. Cache-enabled router 102 receives the request in the form of at least one data packet. Router 102 reads the packet header to determine whether, for example, it is a TCP packet and indicates port 80 as its destination port. If the packet is of a different protocol or is not destined for the World Wide Web, the packet is simply passed through the router and routed according to standard Internet protocols. If, on the other hand, the packet is TCP and port 80 is specified, router 102 determines to which of its associated network caches (108 and 110) it will redirect the packet based on the destination IP address specified in the packet. Before sending the packet to one of its associated network caches, router 102 encapsulates the packet for transmission to the selected network cache by adding another TCP/IP header which designates the router as the source of the packet and the network cache as the destination. That is, the router encapsulates the packet for transmission to a network cache which might be several "hops" away. So, for example, router 102 might encapsulate the packet for transmission to network cache 114 which is connected to router 102 via router 112. Thus, not only may multiple network caches be

Art Unit: 2154

associated with a particular router, but multiple routers may be supported by an individual network cache or a group of network caches. This allows a tremendous amount of flexibility in where the network cache and router need to be in relation to each other. It will, of course, be understood that the present invention is not limited to port 80 or any particular packet encapsulation scheme (e.g., GRE, MAC, etc.) A TCP connection is established between the client and the selected network cache and router 102 transmits the encapsulated packet to the network cache."

Thereby Shaffer teaches a concept that is of a paramount importance to one having ordinary skill in the art. And that that a device can determine whether to apply any encapsulation scheme to the incoming communication by reading the packet header to determine whether, for example, it is a TCP packet. If the packet is of a different protocol or is not destined for the World Wide Web, the packet is simply passed through and routed according to standard Internet protocols. Port 80 and encapsulation scheme are not limitations for applying the concept and technique taught by Shaffer. Thus Shaffer teaches encapsulation in a generic routing format and authentication information is part of generic routing format such as GRE.

Therefore, it would have been an obvious to one of an ordinary skill in art, having the teachings of Bhaskaran and Shaffer in front of him at the time of invention was made, to implement the technique of Shaffer to the flow switch of Bhaskaran such that which can be implemented regardless of the port as well as encapsulation scheme, such as GRE, IPSEC, to selectively send the packets to the server for the network communications requiring end-to-end secure network communications along with the

Art Unit: 2154

load balancing. If the network communication does not require end-to-end secure network communications there is saving in the consumption of valuable processing resources at the flow switch as well as at the destination server level.

**Referring to claims 8 and 9,**

Keeping in mind the teachings of Bhaskaran as stated above, Bhaskaran fails to teach a method according to Claim 5, farther comprising establishing common IP filters for communication at the distribution processor and the plurality of target hosts, and method according to Claim 8, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

Shaffer teaches at col. 5, line 45 -col. 6, line 13, "During normal operation, a client platform 100 transmits a request to retrieve data such as, for example, a multimedia object from destination platform 106. Cache-enabled router 102 receives the request in the form of at least one data packet. Router 102 reads the packet header to determine whether, for example, it is a TCP packet and indicates port 80 as its destination port. If the packet is of a different protocol or is not destined for the World Wide Web, the packet is simply passed through the router and routed according to standard Internet protocols. If, on the other hand, the packet is TCP and port 80 is specified, router 102 determines to which of its associated network caches (108 and 110) it will redirect the packet based on the destination IP address specified in the packet. Before sending the packet to one of its associated network caches, router 102 encapsulates the packet for transmission to the selected network cache by adding another TCP/IP header which designates the router as the source of the packet and the

Art Unit: 2154

network cache as the destination. That is, the router encapsulates the packet for transmission to a network cache which might be several "hops" away. So, for example, router 102 might encapsulate the packet for transmission to network cache 114 which is connected to router 102 via router 112. Thus, not only may multiple network caches be associated with a particular router, but multiple routers may be supported by an individual network cache or a group of network caches. This allows a tremendous amount of flexibility in where the network cache and router need to be in relation to each other. It will, of course, be understood that the present invention is not limited to port 80 or any particular packet encapsulation scheme (e.g., GRE, MAC, etc.) A TCP connection is established between the client and the selected network cache and router 102 transmits the encapsulated packet to the network cache."

Thereby Shaffer teaches a concept that is of a paramount importance to one having ordinary skill in the art. And that that a device can determine whether to apply any encapsulation scheme to the incoming communication by reading the packet header to determine whether, for example, it is a TCP packet. If the packet is of a different protocol or is not destined for the World Wide Web, the packet is simply passed through and routed according to standard Internet protocols. Port 80 and encapsulation scheme are not limitations for applying the concept and technique taught by Shaffer. Thus Shaffer teaches a method according to Claim 5, farther comprising establishing common IP filters for communication at the distribution processor and the plurality of target hosts, and method according to Claim 8, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

Therefore, it would have been an obvious to one of an ordinary skill in art, having the teachings of Bhaskaran and Shaffer in front of him at the time of invention was made, to implement the technique of Shaffer to the flow switch of Bhaskaran such that which can be implemented regardless of the port as well as encapsulation scheme, such as GRE, IPSEC, to selectively filter out the packets to the server for the network communications requiring end-to-end secure network communications along with the load balancing. If the network communication does not require end-to-end secure network communications there is saving in the consumption of valuable processing resources at the flow switch as well as at the destination server level.

**Referring to claim 22,**

Claim 22 is a claim to a system that carries out the method of claim 3. Therefore, claim 22 is rejected for the reasons set forth for claim 3. (please note that means are identified in claim 3).

**Referring to claim 23,**

Claim 23 is a claim to a system that carries out the method of claim 4. Therefore, claim 23 is rejected for the reasons set forth for claim 4. (please note that means are identified in claim 4).

**Referring to claims 24 and 25,**

Claim 24 and 25 are claims to a system that carries out the method of claims 5 and 6. Therefore, claims 24 and 25 are rejected for the reasons set forth for claims 5 and 6. (please note that means are identified in claim 5).

**Referring to claims 27 and 28,**



Claim 27 and 28 are claims to a system that carries out the method of claims 8 and 9. Therefore, claims 27 and 28 are rejected for the reasons set forth for claims 8 and 9. (please note that means are identified in claim 8).

**Referring to claim 41,**

Claim 41 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 3. Therefore, claim 41 is rejected for the reasons set forth for claim 3.

**Referring to claim 42,**

Claim 42 is a claim to a computer readable medium having computer readable program code that carries out the method of claim 4. Therefore, claim 42 is rejected for the reasons set forth for claim 4.

**Referring to claims 43 and 44,**

Claims 43 and 44 are claims to a computer readable medium having computer readable program code that carries out the method of claims 5 and 6. Therefore, claims 43 and 44 are rejected for the reasons set forth for claims 5 and 6.

**Referring to claims 46 and 47,**

Claims 46 and 47 are claims to computer readable medium having computer readable program code that carries out the method of claims 8 and 9. Therefore, claims 46 and 47 are rejected for the reasons set forth for claims 8 and 9.

***Conclusion***

**Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Art Unit: 2154

Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A. Follansbee can be reached on (571) 272-3964. The fax phone

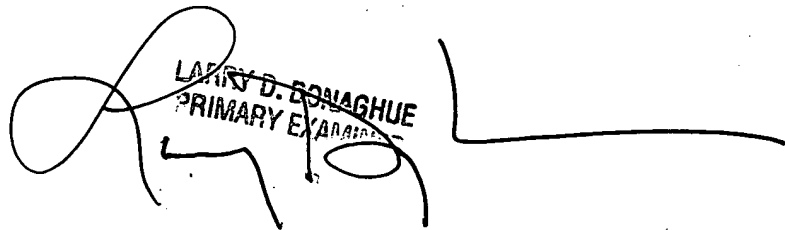
Art Unit: 2154

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abp

\*\*\*

A handwritten signature in black ink, appearing to read 'Larry D. Donaghue', is written over a rectangular stamp. The stamp contains the text 'LARRY D. DONAGHUE' and 'PRIMARY EXAMINER' in a bold, sans-serif font. The signature is fluid and stylized, with a long horizontal line extending to the right.